Some Solutions to HW03 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW03, Problem 2c,2d,2e

Give a 3×3 matrix N that CANNOT be used for the matrix cipher. Apply it to FBI. HEY, that worked- so WHY CAN"T you use it for matrix cipher.

HW03, Problem 2c,2d,2e

Give a 3×3 matrix N that CANNOT be used for the matrix cipher. Apply it to FBI. HEY, that worked- so WHY CAN"T you use it for matrix cipher.

SOLUTION

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Det is 0 which is not rel prime to 26.

If apply to FBI $= (5,1,8)$ we get

$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$

$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$

$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$

So get (14,14,14) which is (O,O,O) (those are letters-O not number-0).

HW03, Problem 2c,2d,2e

Give a 3×3 matrix N that CANNOT be used for the matrix cipher. Apply it to FBI. HEY, that worked- so WHY CAN"T you use it for matrix cipher.

SOLUTION

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Det is 0 which is not rel prime to 26.
If apply to FBI = (5,1,8) we get
$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$
$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$
$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$
So get (14,14,14) which is (O,O,O) (those are letters-O not number-0).
Can't use it since may have TWO string that map to the same string, so cannot decode.

HW03, Problem 2c,2d,2e

Give a 3×3 matrix N that CANNOT be used for the matrix cipher. Apply it to FBI. HEY, that worked- so WHY CAN"T you use it for matrix cipher.

SOLUTION

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Det is 0 which is not rel prime to 26.

If apply to FBI $=$ (5,1,8) we get

$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$

$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$

$1 \times 5 + 1 \times 1 + 1 \times 8 \pmod{26} \equiv 14 \pmod{26}$

So get (14,14,14) which is (O,O,O) (those are letters-O not number-0).

Can't use it since may have TWO string that map to the same string, so cannot decode.

In this case (7,7,0) maps to (14,14,14).

HW03, Problem 3, Set Up

Assume that

- Testing if an $n \times n$ matrix is invertible takes an^3 nsecs.
- The IS-ENGLISH program on a text of length m takes bm nsecs.
- The number of $n \times n$ matrices that are invertible is $c26^{n^2}$. (Note that $c < 1$.)
- Applying an $n \times n$ matrix to a vector of length n takes dn nsecs.
- The dot product of two length n vectors takes en nsecs. (Note that e is NOT the e from calculus.)

HW03, Problem 3a

How many nsecs does the matrix-brute force alg take to crack the $n \times n$ matrix cipher if you have a text of length m? The answer should be in terms of a, b, c, d, n, m and NOT have any O-of terms. (Assume that n divides m.)

HW03, Problem 3a

How many nsecs does the matrix-brute force alg take to crack the $n \times n$ matrix cipher if you have a text of length m? The answer should be in terms of a, b, c, d, n, m and NOT have any O-of terms. (Assume that n divides m.)

SOLUTION

You have to to look at 26^{n^2} matrices. For each one you have to test invertible: an^3. So $an^3 26^{n^2}$.

For all inv $c26^{n^2}$ matrices, apply M to T and apply IS-ENGLISH.

- Text is $\frac{m}{n}$ blocks of length n. Apply M to a vector $\frac{m}{n}$ times: $\frac{m}{n}dn = dm$.
- IS-ENGLISH takes bm steps. Hence this takes $c26^{n^2}(dm + bm) = (d + b)mc26^{n^2}$ nsecs.

$$an^3 26^{n^2} + (b + d)mc26^{n^2} = (an^3 + bmc + dmc)26^{n^2}.$$

HW03, Problem 3c

How many nsecs does the row-brute force alg take to crack the $n \times n$ matrix cipher if you have a text of length m? The answer should be in terms of a, b, c, d, n, m and NOT have any O-of terms. (Assume n divides m.)

HW03, Problem 3c

How many nsecs does the row-brute force alg take to crack the $n \times n$ matrix cipher if you have a text of length m? The answer should be in terms of a, b, c, d, n, m and NOT have any O-of terms. (Assume n divides m.)

SOLUTION

There are n rows. For each row there are 26^n possibilities. We will be doing the following for each guess of each row, so we multiply the time for the following by $n26^n$:

Multiply the row by each of the $\frac{m}{n}$ block of length n. This takes $\frac{m}{n}en = em$ steps.

Apply IS-ENGLISH to every rth letter that was decoded by the rth row. This takes $b\frac{m}{n}$ nsecs.

Hence the entire process takes $(en + b)m26^n$ nsecs.

HW03, Problem 4a

Alice and Bob are using a 3×3 matrix cipher. Eve knows from yesterdays message and what happened that FDR is coded as WHH

Write down the equations that Eve will obtain to help her crack the cipher.

HW03, Problem 4a

Alice and Bob are using a 3×3 matrix cipher. Eve knows from yesterdays message and what happened that FDR is coded as WHH

Write down the equations that Eve will obtain to help her crack the cipher.

SOLUTION

Assume matrix is:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

FDR is 5,3,17. WHH is 22,7,7.

Hence the equations are

$5a + 3b + 17c = 22$

$5d + 3e + 17f = 7$

$5g + 3h + 17i = 7$

HW03, Problem 4b

Alice and Bob are using a 3×3 matrix cipher. How many plaintext-ciphertext pairs does Eve have to know in order to crack the cipher?

HW03, Problem 4b

Alice and Bob are using a 3×3 matrix cipher. How many plaintext-ciphertext pairs does Eve have to know in order to crack the cipher?

SOLUTION

Each pair gives 3 equations. Since there are 9 variables we need 9 equations. Hence we need 3 pairs.

HW03, Problem 4c

Assume Eve uses an $n \times n$ matrix code. How many plaintext-ciphertext pairs does Eve to have know in order to crack the cipher?

HW03, Problem 4c

Assume Eve uses an $n \times n$ matrix code. How many plaintext-ciphertext pairs does Eve to have know in order to crack the cipher?

SOLUTION

Each pair gives n equations. There are n^2 variables, so we need n^2 equations. Hence we need n pairs.

HW03, Problem 4d

Assume Eve has one less plaintext-ciphertext than she needs to crack the cipher. Can she still, with some cleverness and guesswork, crack the cipher?

HW03, Problem 4d

Assume Eve has one less plaintext-ciphertext than she needs to crack the cipher. Can she still, with some cleverness and guesswork, crack the cipher?

SOLUTIONS

The equations will give Eve constraints on what the entries in the matrix will be. The number of possible matrices is small— so Eve can guess each option and then use IS-ENGLISH.